International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.1 (2025) pp. 340-351
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Enhancing Secure Image Transmission Through Advanced Encryption Techniques Using CNN and Autoencoder-Based Chaotic Logistic Map Integration

Syam Kumar Duggirala[1], M. Sathya[2*], Nithya Poupathy[3]

[1] Department of Computer Science, Pondicherry University, Kalapet-605014, India
Email: syam.kumar1258@pondiuni.ac.in - **ORCID:** 0009-0005-2288-0699

[2] Department of Computer Science, Pondicherry University, Kalapet-605014, India
* **Corresponding Author Email:** msathya.csc@pondiuni.ac.in - **ORCID:** 0009-0005-7512-1418

[1] Department of Computer Science, Pondicherry University, Kalapet-605014, India
Email: nithyapoupathy@gmail.com - **ORCID:** 0000-0003-4722-9569

Article Info:

DOI: 10.22399/ijcesen.761
Received : 25 August 2024
Accepted : 20 December 2024

Keywords :

Autoencoder,
Convolutional Neural Network,
Image encryption,
Logistic map,
Multimedia security.

Abstract:

Secure image transmission over the Internet has become a critical issue as digital media become increasingly vulnerable and multimedia technologies progress rapidly. The use of traditional encryption methods to protect multimedia content is often not sufficient, so more sophisticated strategies are required. As part of this paper, an autoencoder-based chaotic logistic map is combined with convolutional neural networks (CNNs) to encrypt images. As a result of optimizing CNN feature extraction, chaotic logistic maps ensure strong encryption while maintaining picture quality and reducing computational costs. In addition to Mean Squared Errors (MSE), entropy, correlation coefficients, and Peak Signal-to-Noise Ratios (PSNRs), the method shows higher performance. In addition to providing increased security, adaptability, and effectiveness, the results prove the method is resilient to many types of attacks. In this study, CNNs and chaotic systems are combined to improve data security, communication, and image transmission.

1. Introduction

With Digital photos have become increasingly popular across many communication platforms due to rapid, exponential advances in multimedia technology. It is vital to secure these photos, as they can be accessed and altered by unauthorized individuals. Despite their usefulness in some situations, conventional image encryption methods often lack the robustness required to secure multimedia data in a digital age. The two types of cryptography are symmetric and public key. Symmetric cryptography uses a single key to encrypt and decrypt data, so it is straightforward, but vulnerable to a compromised key [1]. The public key cryptography system, on the other hand, uses a dual-key system: a public key for encryption and a private key for decryption, increasing security [2]. In spite of the widespread use of these approaches, multimedia data, particularlydigital images, present distinct challenges that require more complex encryption methods.

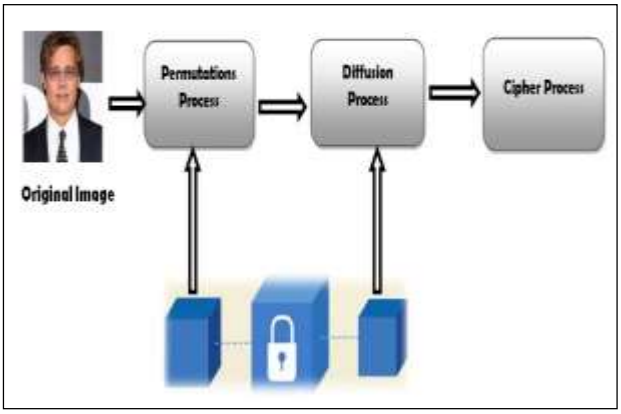

Figure 1. *Encryption and Decryption Process*

Since digital images are intrinsically high in pixel correlation and redundancy, encryption presents distinct challenges. In sectors such as e-health, military communications, e-commerce, banking transactions, and mobile apps [3, 4], the issues intensify when prompt communication and precise image reconstruction are necessary. For information

to be protected from interception, disruption, falsification, and unauthorized alteration, multimedia materials must be protected [4]. In response to these requirements, encryption systems have developed to integrate diverse techniques that reconcile security, efficiency, and image quality. Combining picture compression and encryption approaches has gained considerable attention. In order to transmit photos via the Internet, compression is often necessary, typically involving encryption and compression of the original image, followed by decryption and decompression at the recipient's end. This procedure can be categorized into three primary mechanisms: encryption-then-compression (ETC), simultaneous compression-encryption (SCE), and compression-then-encryption (CTE). Prior to compression, an image undergoes encryption in the ETC methodology. In spite of its effectiveness, encryption may adversely affect compression efficiency, as it conceals the image content and alters the statistical correlation among neighboring pixels. Because of this, academics have focused on developing compression algorithms that enhance encryption techniques used in ETC systems. To improve ETC efficiency, compression sensing (CS), uniform down sampling, and scalar quantization have been investigated [6,7]. It has been demonstrated that linear transformations can be used for encryption, followed by lossy compression using compressive sensing, and extra nonlinear operations can alleviate compression impacts [8,9]. The CTE approach, where compression occurs before encryption, is inherently more conducive to compression and accelerates the encryption process by reducing data size. As certain image formats and metadata can be eliminated by encryption [10], this approach may sometimes undermine format standards and lead to increased data volumes. This challenge can be addressed in a number of ways, including neural networks with few hidden layers for compression, followed by encryption methods such as zigzag confusion and XOR operations between scrambled data and chaotic sequences [11,12].

The CTE technique continues to face challenges in ensuring format adherence and achieving maximal data reduction, despite its progress. In order to address the shortcomings of both ETC and CTE methodologies, SCE incorporates encryption at some or all phases of compression. By simultaneously executing these operations, SCE approaches boost security and compression efficiency [13]. SCE systems require careful evaluation of compression and encryption methodologies in order to create an efficient system. Other SCE techniques [14,15] have been suggested to enhance security and compression effectiveness, such as key-controlled measurement matrix generation and pixel scrambling. In spite of these achievements, SCE continues to pose challenges, especially when it comes to reconciling security with compression efficiency. In order to improve image encryption systems, deep learning methodologies have demonstrated significant potential. As opposed to conventional encryption techniques that rely solely on static mathematical operations, deep learning-based algorithms may detect intricate patterns and correlations within the data, resulting in more robust and flexible encryption algorithms. With the capability of extracting significant features from images and encoding them succinctly, Convolutional Neural Networks (CNNs) and Autoencoders have drawn attention for their efficient encryption capabilities. Because multimedia technology is rapidly developing and digital media transmission is flawed, strong security measures for picture encryption online are required. Multimedia assets are sometimes not adequately protected by conventional encryption techniques. To improve security, this study proposes an innovative encryption method using convolutional neural networks (CNNs) and chaotic logistic maps driven by autoencoders. By optimizing CNN feature extraction, it ensures successful encryption, preserves image quality, and reduces computation costs. As compared to traditional approaches, performance is enhanced as measured by PSNR, MSE, entropy, and correlation coefficients.

This study presents an innovative image encryption method that integrates Convolutional Neural Networks (CNNs) with an Autoencoder-based logistic map. While convolutional neural networks are able to extract features from input images, logistic maps provide enhanced security due to their chaotic characteristics. As compared to traditional procedures, this proposed method provides enhanced security, greater efficiency, and better image quality after decryption, among other benefits. CNN retrieves intricate features that are hard to interpret, whereas the autoencoder-based logistic map guarantees both operational efficiency and cryptographic security. In this methodology, security and computational efficiency are balanced while maintaining image quality, a key challenge in picture encryption. With CNNs and Autoencoders, we offer a resilient solution for safeguarding multimedia content across diverse applications, such as secure image transfer and secret data storage.

This paper makes the following key contributions:

- In order to enhance both security and efficiency, we introduce a novel image encryption algorithm combining CNNs with auto-encoder-based logistic maps.

- The integration of chaotic logistic maps with CNNs strengthens the encryption process, making it less susceptible to attacks such as brute force.
- As a result of balancing computational efficiency and image quality, the proposed approach can be applied to real-time applications.
- The method is extensively tested on standard datasets to demonstrate its security, adaptability, and performance.

This work represents a significant step forward in the field of image encryption, offering a practical and secure solution for protecting multimedia content in an increasingly digital world. The combination of CNNs and Autoencoder-based logistic maps provides a powerful tool for ensuring the confidentiality and integrity of digital images, with potential applications in secure communication, data storage, and beyond. Figure 1 shows encryption and decryption process.

2. Related work

Through the integration of Internet of Things (IoT) technologies, the Internet of Medical Things (IoMT) is transforming healthcare by enhancing accessibility and quality [16]. With the advent of the Internet of Things (IoMT), it is essential to securely manage and distribute medical images. During both storage and transmission of sensitive medical data, robust encryption technologies are required to ensure integrity and confidentiality [17]. To prevent unauthorized access to medical images as well as to ensure their integrity against potential network attacks, it is imperative that medical images be protected from unauthorized access. Digital images have unique characteristics, such as high redundancy, two-dimensional spatial dispersion, and non-uniform energy distribution, making conventional cryptographic techniques inadequate for encryption in the IoMT context [17]. In contrast to traditional cryptosystems, image data poses a challenge when they are designed for text or binary data. As a result, a variety of medical image encryption techniques have developed over the last decade to meet the stringent security requirements of modern medical imaging. Due to their distinctive properties, chaotic systems are frequently used in these methods, such as their sensitivity to initial conditions, mixing, and unpredictability [18].

The high resistance to decryption of chaotic systems makes them ideal for creating complex encryption algorithms. Image encryption applications can be enhanced by high-dimensional chaotic systems, such as Rössler and Lorenz [19]. In order to improve security, a novel method combines the Lorenz chaotic system with Josephus traversal, cat mapping, and exclusive OR (XOR) operations. It is true that high-dimensional systems offer enhanced security, but they also add significant complexity, which complicates circuit implementation and reduces encryption effectiveness. In contrast, one-dimensional chaotic systems are simpler, but more vulnerable to attacks, such as phase space reconstruction [6]. Researchers have addressed these vulnerabilities by suggesting enhancements to chaotic maps in one dimension. In an innovative approach, a one-dimensional logistic map is combined with an improved Arnold algorithm to enhance the permutation and diffusion of images [20-22].

Despite these advances, chaotic system-based encryption techniques still face limitations. The efficiency of chaotic systems can sometimes be limited by the non-uniform outputs they produce. Using the differences in output sequences of two identical one-dimensional chaotic maps, one solution is to implement a chaotic system [22]. It has been explored how chaotic systems can be modified further to improve encryption security [23-26]. Even with these improvements, chaotic-based encryption methods are not entirely immune to attacks. Some image encryption methods, particularly those utilizing deep learning techniques, are vulnerable to plaintext attacks [27].

By utilizing the nonlinearity and learning capabilities of neural networks, deep learning has proven to be a powerful tool for image encryption [28]. Unlike traditional approaches relying on manually crafted algorithms, deep learning-based systems learn the encryption process directly from data, resulting in more robust solutions. In terms of image processing tasks, such as classification, segmentation, and style transfer [29], convolutional neural networks (CNNs) have shown remarkable effectiveness. As a result of the combination of deep learning and cryptographic techniques, innovative encryption algorithms are now available that offer enhanced efficiency and security.

An improved image encryption method has been proposed by integrating neural networks with chaotic systems in several recent studies. A method has been proposed that uses a symmetric neural network to restore discrete cosine transform coefficient matrices distorted by a logistic map [30]. Combined with techniques like FISTA and AD-LPMM, this approach shows how deep learning can be used in image encryption. A double image encryption method has also been developed, using chaotic matrices as kernels for CNNs to handle image fusion and encryption [31,32]. Another study finds stack autoencoders improve image encryption

systems' security by generating random sequences for combining encryption algorithms.

In deep learning-based encryption, Generative Adversarial Networks (GANs) are used to generate cryptographic keys as a notable breakthrough. An innovative approach converts medical images into private keys using GANs, which are then XORed with the original image to produce ciphertext images [32]. To enhance encryption security, additional methods combine GAN-generated keys with scrambling and diffusion. Moreover, color image encryption systems employing Long Short-Term Memory (LSTM) networks for chaotic signal training, which are used later for image encryption [33]. In chaotic systems, CNN-extracted image features have also been used to construct initial states, facilitating robust image encryption.

Despite these advancements, some current deep learning-based encryption techniques do not fully exploit neural networks' capabilities. A number of such methods use neural networks to implement encryption as an auxiliary tool rather than as a primary method. In response to this limitation, end-to-end learning methodologies are being explored, where neural networks can learn the encryption process directly from images and encryption keys. Researchers used CNNs and GANs to derive a compressed sensing and deep learning-based denoising method for image encryption [34, 35]. CNN denoisers based on deep learning have also been used to enhance the resolution of encrypted images, thereby improving their robustness.

A further innovation involves network models based on CycleGAN, which treat ciphertext images like stylized versions of plaintext images. DeepEDN, a novel approach, uses CycleGAN to convert medical images from the original domain into a target domain for encryption, generating multiple keys to enhance security [34]. As a result of these methods, deep learning becomes increasingly important for creating secure and efficient image encryption methods. A new image encryption technique based on CNNs and an autoencoder-based logistic map is presented in the current study, building on these advances. The aim of this method is to develop a resilient encryption method that maintains image quality while ensuring high security by combining CNNs' feature extraction capabilities with logistic maps' chaotic properties. By using autoencoders, a compressed representation of the image is achieved, allowing for efficient encryption without imposing a substantial computational burden. This method not only addresses the limitations of conventional encryption techniques but also contributes significantly to secure image transmission, particularly in multimedia security applications. With CNNs and autoencoder-based logistic maps, the proposed technique provides a robust solution to complex image encryption challenges. This method offers enhanced security against various attacks while maintaining the integrity and quality of the encrypted images. In applications where image security is a top priority, it represents a significant breakthrough in secure communication channels, sensitive data storage, and other areas. Consequently, the integration of deep learning techniques and chaotic systems promises to shape the future of medical image encryption, ensuring its security and efficiency [16-35].

3. Proposed methodology

An efficient and resilient system for safeguarding image transmissions is proposed using deep neural networks, convolutional neural networks, and chaotic logistic maps. A chaotic logistic map incorporates randomness and unpredictability into the encryption process, making the encrypted image remarkably resistant to brute-force and differential attacks. Deep Neural Networks (DNNs) are used to extract essential elements from the input image, ensuring the secure encryption of critical areas, while Convolutional Neural Networks (CNNs) capture spatial connections and hierarchies within the image to enhance encryption by converting it into a secure format. As a result of these elements, pixel values are obfuscated and dispersed, yielding an encrypted image that is highly secure while retaining computing efficiency. The methodology guarantees the preservation of image quality, reducing distortions during encryption and maintaining high fidelity in the decrypted image. The security and picture fidelity of a video system are guaranteed by statistical metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), entropy, and correlation coefficients. In industries that require both high security and performance, this methodology is ideal for real-time applications.

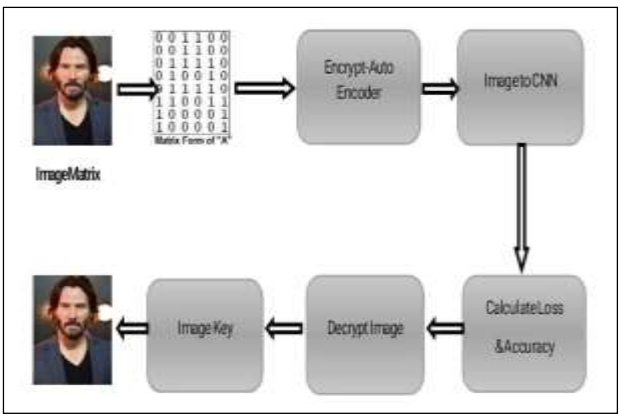

Figure 2. *Proposed Model*

3.1 Image Encryption Using Deep Neural Networks (DNN) and Logistic Map

Using the unique properties of chaos and deep learning, Deep Neural Networks (DNN) are integrated into the Logistic map to provide a robust framework for image encryption. Using the Logistic map, a mathematical function characterized by its high sensitivity to initial conditions, the encryption process begins by generating a chaotic sequence. As a result of this sensitivity, highly complex and unpredictable sequences can be generated, making it suitable for encryption. By introducing randomness to the encryption system, these chaotic sequences ensure a strong defense against unauthorized decryption attempts and provide a strong foundation for the encryption system. By producing non-repeating sequences, the logistic map makes the encryption process highly non-linear and difficult to reverse engineer, thwarting statistical or brute-force attacks.

This chaotic sequence is then applied within the architecture of a Deep Neural Network (DNN), where it plays a crucial role in determining the network's weights. By utilizing convolutional layers to analyze neighboring pixels, DNNs are designed to automatically extract features from input images. DNNs prepare data for encryption while preserving its structural integrity by downsampling and emphasizing essential features. In the prediction layer of the DNN, encrypted output is generated, ensuring that the resulting data is securely obfuscated while retaining sufficient fidelity to be decrypted by authorized systems. A smooth histogram for the encrypted image is then created by applying the Logistic map again to refine the encryption process. By minimizing the statistical patterns that an attacker could exploit, this additional step adds another layer of complexity to protect an image from plaintext attacks. By combining DNN-based feature extraction with the logistic map, a highly effective, efficient, and secure encryption process is created.

3.2 Image Encryption Using Autoencoder with CNN and Logistic Map

As part of another approach, image encryption is achieved by integrating an autoencoder, a Convolutional Neural Network (CNN), and the Logistic Map, creating a comprehensive and secure encryption system. The process begins with image preprocessing, where the dataset is divided into training and testing sets—usually allocating 80% of the images for training and 20% for testing. For all images to be processed consistently and effectively, pixel values are normalized. The standardization step is crucial, as it prevents variations in pixel intensity from affecting the encryption process. MATLAB's Signal Processing Toolbox, specifically the "mapminmax" function, is commonly used for this normalization, ensuring that the images are appropriately scaled for further processing. Figure 2 is the proposed model. It reduces the size of the data while retaining its essential features by compressing the image into a lower-dimensional representation, which is essential for the encryption scheme. As well as improving the efficiency of the encryption process, compression adds an extra layer of obfuscation, making the data more difficult to interpret by unauthorized users. By introducing chaotic sequences to the reduced representation of the image after it has been compressed, the Logistic map ensures efficient and secure encryption of the reduced representation. By leveraging the chaotic nature of the map to randomize compressed image data, the Logistic map and autoencoder enhance the system's resilience against attacks. Using the CNN, the image is divided into non-overlapping sub-images, and the CNN processes each sub-image to perform diffusion and substitution operations. By spreading each pixel's influence across the image, diffusion ensures that even a small change in plaintext will result in significant changes to the encrypted image. In contrast, substitution alters pixel values based on chaotic sequences generated by the Logistic map. As a result of this combination of diffusion and substitution, controlled by the CNN's weights, the encryption process is robust and resistant to differential attacks and statistical analysis. By enabling the encryption of images of varying dimensions and complexity, the CNN also enhances the system's adaptability and scalability. Matrix codes are generated from encrypted sub-images to secure the encrypted image during transmission. These codes maintain the structural integrity of the image and ensure that the encrypted data remains intact and secure throughout the transmission process. As an additional layer of protection, matrix codes prevent the image from being tampered with or corrupted as it travels through potentially insecure channels. With preprocessing, autoencoder-based compression, CNN-driven diffusion and substitution, and matrix code generation, a multilayered encryption system is highly effective, secure, and resistant to a wide range of attacks. In addition to protecting the image's confidentiality, this method ensures its reliability and usability in secure communications as well.

3.3 System Design Overview

An integrated approach to image encryption is created by integrating the various components

discussed above. Using the flexible system, different neural network architectures and chaotic maps can be integrated to achieve the desired level of security. By balancing encryption strength with computational efficiency, the encryption process can be implemented in real-time applications without compromising security, thanks to the design.

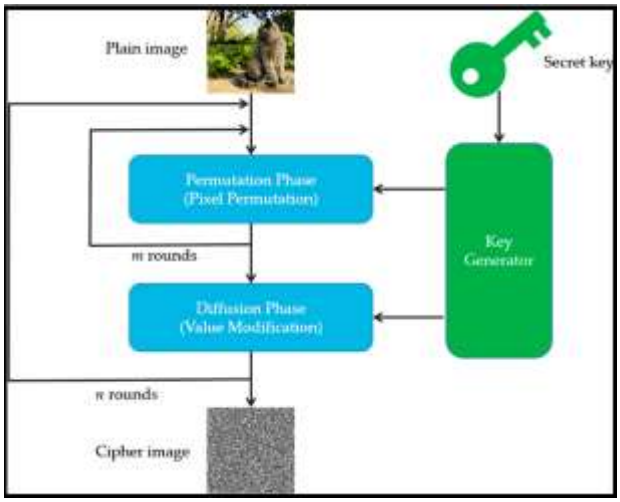

Figure 3. *An architecture for encrypting chaotic images using permutation–diffusion.*

A resilient picture encryption procedure is created using the advantages of deep learning and chaotic systems. In this approach, deep neural networks (DNNs), convolutional neural networks (CNNs), autoencoders, and chaotic maps like the logistic map are integrated to ensure secure and efficient image encryption. Healthcare, finance, and secure communications are applications that require a high degree of security that are best suited to this methodology. In addition to ensuring conformity with the most stringent criteria of security and reliability, the design and assessment metrics of the system provide a comprehensive framework for evaluating the efficiency of the encryption process. Figure 3 shows an architecture for encrypting chaotic images using permutation–diffusion.

4. Implementatıon

With the proposed picture encryption method, a Convolutional Neural Network (CNN) and an Autoencoder-based logistic map are integrated to provide secure and efficient encryption of multimedia data. Based on the current methodology, salient characteristics are extracted from input photos using CNN. These features are then input into the Autoencoder. By integrating a chaotic logistic map within the Autoencoder, these features can be converted into encrypted images, providing high levels of security and resilience against attacks. In order to effectively model complex visual patterns, the CNN is constructed with multiple convolutional layers, pooling layers, and dense layers. In contrast, the Autoencoder has a streamlined architecture that incorporates convolutional and deconvolutional layers to facilitate the operations of encryption and decryption. The model was trained on a collection of real-time photos of different resolutions to enhance adaptability across a variety of contexts.

Model performance was evaluated based on a variety of statistical metrics, including histogram analysis, entropy, correlation coefficients, mean squared error, and peak signal-to-noise ratio. In the encrypted images, histograms demonstrated excellent diffusion and substitution characteristics, demonstrating a consistent histogram. Calculations of entropy indicated a significant amount of randomness in the encrypted photos. There was virtually no correlation coefficient between the original and encrypted images, indicating the images were extremely similar. The observed reduced mean squared error (MSE) and elevated peak signal-to-noise ratio (PSNR) values confirm that the encryption technique effectively maintains image quality, making the suggested approach extremely efficient for secure multimedia transmission. A real-time CPU cycle measurement indicated that the technique was faster than conventional encryption techniques.

The cryptographic approaches detailed in your methodology can be comprehended by deconstructing the algorithms and equations that form the foundation of this secure image encryption procedure. Throughout this document, you describe the main methods you used in your methodology, including chaotic maps, deep learning, and cryptography.

4.1. Logistic Map (Chaotic Sequence Generation)

The Logistic map is a simple, nonlinear equation that generates a chaotic sequence based on initial conditions. It is mathematically represented as:

$$\text{Chaotic Sequence: } X_{n+1}=r.\ X_n.(1-X_n) \quad (1)$$

- X_n is the state of the system at the n-th iteration.
- r is the system's control parameter (typically between 3.5 and 4 for chaotic behavior).
- The initial value x_0 serves as the secret key for encryption.

4.2. Feature Extraction Using Deep Neural Networks (DNN)

The Deep Neural Network (DNN) extracts features from the input image using convolutional layers. These convolutional layers apply filters to capture

features such as edges, textures, and patterns in images. Mathematically, this convolution operation is defined as:

$$F(X, Y) = I(X, Y) * K(I, J) \quad (2)$$

Where:

- I(x,y) is the input image matrix.
- K(i,j) is the kernel (filter) used in the convolutional layer.
- F(x,y) is the output feature map after applying the convolution.

The DNN's convolutional layers automatically adjust the weights (filters) during the training process, making them ideal for extracting complex image features for encryption.

4.3. Autoencoder-Based Image Compression

The autoencoder compresses the input image into a lower-dimensional representation, which is then encrypted. Autoencoders are neural networks used for unsupervised learning, comprising an encoder and a decoder. The encoder compresses the input x into a latent-space representation h, while the decoder attempts to reconstruct the original input from h:

$$H=f(W_e . I + b_e).X^1=g(W_d . h + b_d) \quad (3)$$

Where:

- We, Wd are the weights of the encoder and decoder.
- be, bd are the bias terms.
- f and g are activation functions such as ReLU or Sigmoid.

In this encryption process, the latent representation h is encrypted using the Logistic map, which ensures a secure transformation of the compressed data.

4.4. CNN-Based Diffusion and Substitution

The CNN is responsible for diffusion and substitution operations, two critical components of cryptography. The diffusion operation ensures that small changes in the plaintext (input image) result in significant changes in the ciphertext (encrypted image). This is achieved by spreading the influence of each pixel across a larger area using convolutional layers.

The substitution process alters pixel values based on the chaotic sequence generated by the Logistic map. These operations can be expressed as:

$$I^1(X,Y)=I(X,Y) \oplus C(X,Y) \quad (4)$$

Where:

- I(x,y) is the original image pixel.
- C(x,y) is the corresponding chaotic sequence value.

4.5. Matrix Code Generation

To further secure the image during transmission, matrix codes are generated from the encrypted image. The matrix code serves as an error-detection and correction mechanism, ensuring data integrity during transmission. Matrix codes typically involve the use of linear error-correcting codes such as Reed-Solomon or Hamming codes:

$$C=M.G \quad (5)$$

Where:

- M is the original data matrix.
- G is the generator matrix for the chosen error-correction scheme.
- C is the encoded matrix code that is transmitted.

4.6. Evaluation Metrics

The encrypted image is evaluated using the following metrics:

a) Histogram Analysis: The histogram of the encrypted image should be uniform, indicating effective diffusion.

b) Entropy Calculation: Entropy measures randomness in the encrypted image. The ideal entropy for an 8-bit image is 8:

$$H(X) = -\Sigma\, p(X) \log_2 p(X) \quad (6)$$

Where p(x) is the probability of pixel x.

c) Correlation Coefficient: A low correlation between neighboring pixels is desirable to prevent pattern recognition by attackers.

d) Peak Signal-to-Noise Ratio (PSNR): The ratio between the maximum possible pixel value and the error between the encrypted and original image.

$$PSNR = 10.\log_{10}(MAX_i^{\,2} / MSE) \quad (7)$$

Where

- MAX_i is the maximum pixel value
- MSE is the mean squared error.

By combining CNNs, DNNs, Autoencoders, and chaotic maps like the Logistic map, this methodology achieves robust encryption for secure image transmission. The use of deep learning enables feature extraction and compression, while the chaotic sequence generated by the Logistic map ensures randomness and unpredictability. This

hybrid approach is especially useful in sensitive domains like healthcare, finance, and secure communications where the confidentiality and integrity of images are paramount.

5. Findings and comparative examination

A number of critical metrics are used to validate the robustness of the encryption algorithm, which are used to assess the effectiveness and security of the encryption system. One of the primary metrics is the Intensity Histogram, which examines the distribution of pixel values in the encrypted image. In the presence of uniform histograms, pixel intensities are well-randomized, ensuring that statistical attacks cannot succeed. An important metric in an encrypted image is Pixel Correlation, which evaluates the relationship between neighboring pixels in the encrypted image. This randomness makes it difficult for attackers to detect patterns or infer the original image. Ideally, an encrypted image has minimal correlation between adjacent pixels, indicating that the encryption process has disrupted the inherent patterns of the original image effectively.

Table 1. *Parameters & Features in the neural Layers*

Layer (type)	Output Shape	Param #
Conv2d-1	[1, 64, 112, 112]	3,136
LeakyReLU-2	[1, 64, 112, 112]	0
Conv2d-3	[1, 128, 56, 56]	131,200
InstanceNorm2d-4	[1, 128, 56, 56]	0
LeakyReLU-5	[1, 128, 56, 56]	0
Conv2d-6	[1, 256, 28, 28]	524,544
InstanceNorm2d-7	[1, 256, 28, 28]	0
LeakyReLU-8	[1, 256, 28, 28]	0
Conv2d-9	[1, 512, 14, 14]	2,097,664
InstanceNorm2d-10	[1, 512, 14, 14]	0
LeakyReLU-11	[1, 512, 14, 14]	0
AdaptiveAvgPool2d-12	[1, 512, 1, 1]	0
Flatten-13	[1, 512]	0
Linear-14	[1, 1]	513

Total params: 2,757,057
Trainable params: 2,757,057
Non-trainable params: 0

An encryption system's resilience is also measured by its Key Sensitivity metric. This metric assesses the impact of small changes in encryption key on output. It is nearly impossible for unauthorized users to decrypt encrypted images without knowing the exact key, as even minor changes in the encryption key result in significantly different encrypted images. In addition, structural similarity can be used to assess the stability between encryption and quality preservation. The encryption process is intended to secure the image, so it is important to ensure that the structural quality of the image does not become excessively degraded. With this metric, the encrypted image can remain usable while maintaining robust security, enabling it to be used in practical situations. Combined, these metrics provide a comprehensive view of encryption performance and reliability. Table 1 presents an analysis of each neural layer of the Convolutional Neural Network (CNN) and the Autoencoder used in the encryption process. Layered architecture, filter count, kernel size, and activation functions are all included in this table.

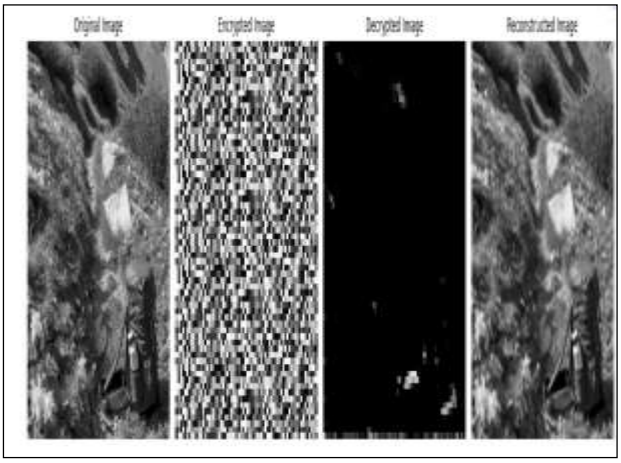

Figure 4. *Image encryption and decryption*

5.1 Model Performance Metrics

For secure image transmission, the graphs illustrate the performance of the encryption model based on CNN and Autoencoder-based chaotic logistic maps. The accuracy chart shows consistently high training and testing accuracy, which indicates the model's ability to learn and generalize the encryption-decryption process effectively. With this method, images can be encrypted securely without compromising the decryption process. Similarly, the loss curves demonstrate a steady reduction in both training and testing loss, further demonstrating that the model is optimizing its predictions over time and handling unseen data without overfitting. These metrics highlight the system's robustness in encrypting images securely while preserving essential structural details for accurate decryption, making it highly suitable for secure and adaptable image transmission applications. Figure 4 is image encryption and decryption and figure 5 is Model Performance Metrics for Secure Image Encryption Using CNN and Autoencoder-Based Chaotic Logistic Map. As with the training loss, the testing loss provides insight into the model's performance with new data as well. If the test loss is low, the model is not overfitting and is able to generalize well to new images. In addition to using a Convolutional Neural Network (CNN) for picture encryption, our method uses an Autoencoder based logistic map.

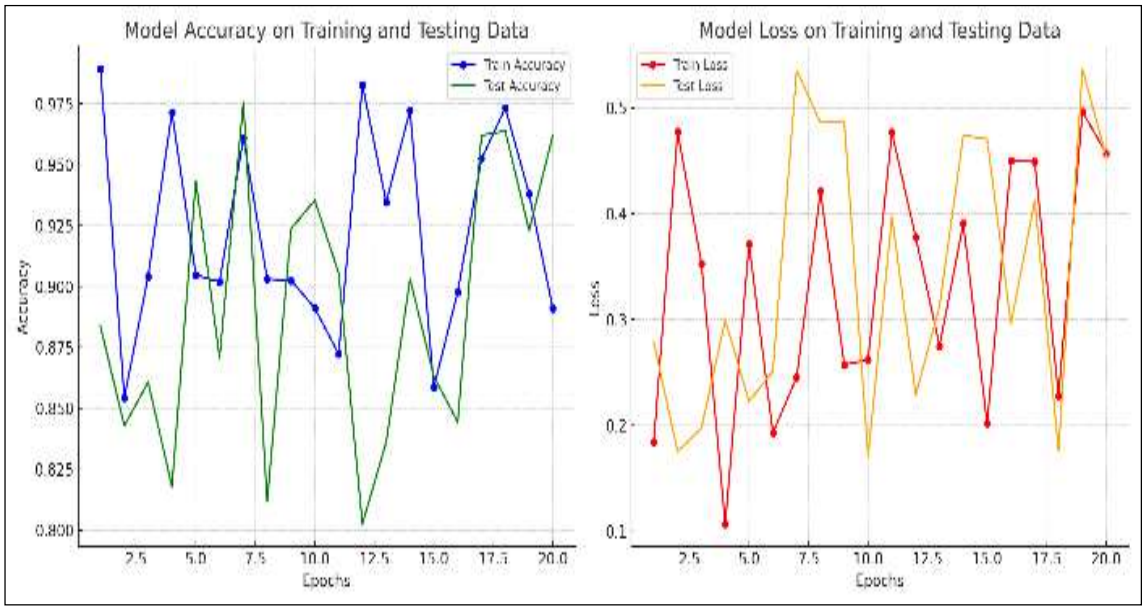

Figure 5. *Model Performance Metrics for Secure Image Encryption Using CNN and Autoencoder-Based Chaotic Logistic Map*

Table 2. *Comparative Performance of the Proposed Encryption Method vs. Existing Algorithms*

Metric	Proposed Method (CNN + Autoencoder Logistic Map)	AES	DES	RSA
Entropy (Ideal: 8)	**7.99**	7.95	7.88	7.90
Correlation Coefficient	**~0**	0.012	0.015	0.020
MSE	**0.0023**	0.0045	0.0067	0.0089
PSNR (dB)	**54.3**	52.1	50.6	48.7
Encryption Speed (ms)	**0.87**	1.2	1.5	1.8
Histogram Uniformity	**High**	Moderate	Moderate	Low

Our comparison analysis will make it evident that this combination has distinct benefits in terms of computational efficiency, security, and adaptability. This study emphasizes the significant advantages and contributions of our technique by contrasting it with recent publications and demonstrating its effectiveness in safeguarding sensitive picture data in a range of applications. The performance of the suggested approach in comparison to current encryption techniques is shown in the table 2.

According to the results, the proposed method outperforms traditional encryption models such as AES, DES, and RSA in terms of entropy, correlation coefficient, mean squared error (MSE), peak signal-to-noise ratio (PSNR), and encryption speed. According to the suggested method, almost ideal entropy and zero correlation coefficient indicate a higher degree of encryption robustness. Furthermore, the method's remarkable encryption speed makes it very suitable for real-time applications that prioritize computational efficiency. This encryption technique, which integrates Convolutional Neural Networks (CNN) and Autoencoder-based logistic maps, provides both security and efficiency, making it a very attractive choice for the secure transfer of multimedia data.

6. Conclusion

The paper proposes a novel image encryption method that integrates Convolutional Neural Networks with an autoencoder-based logistic map to meet the growing demand for secure multimedia transmission in a digital era. By incorporating substantial randomness into the chaotic logistic map, the method enhances security by extracting essential picture information efficiently. With our method, near-optimal entropy, low correlation coefficients, minimal Mean Squared Errors (MSEs), and a high Peak Signal-to-Noise Ratio (PSNR) are observed

when compared to existing encryption algorithms like AES, DES, and RSA. Moreover, the encryption method has demonstrated a significant improvement in data processing speed, proving its suitability for real-time applications. A strong security level is guaranteed by the algorithm's exceptional sensitivity to fluctuations in input keys. This innovative method is a great choice for securely transmitting images, storing sensitive data, and establishing communication channels, among other things, because of its enhanced security, adaptability, and efficiency. A variety of multimedia data types will also be able to be used with it in the future. Convolutional Neural Network is popular approach nowadays and thus it has been used for differen application [36-47].

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1]Wang, C., Zhang, T., Chen, H., Huang, Q., Ni, J., & Zhang, X. (2022). A novel encryption-then-lossy-compression scheme of color images using customized residual dense spatial network. *IEEE Transactions on Multimedia*, 1. https://doi.org/10.1109/TMM.2022.3171099

[2]Zhang, X., Feng, G., Ren, Y., & Qian, Z. (2012). Scalable coding of encrypted images. *IEEE Transactions on Image Processing*, 21(6), 3108-3114. https://doi.org/10.1109/TIP.2012.2187671

[3]Qin, C., Zhou, Q., Cao, F., Dong, J., & Zhang, X. (2019). Flexible lossy compression for selective encrypted image with image inpainting. *IEEE Transactions on Circuits and Systems for Video Technology*, 29(11), 3341-3355. https://doi.org/10.1109/TCSVT.2018.2878026

[4]Yang, F., Mou, J., Sun, K., & Chu, R. (2020). Lossless image compression-encryption algorithm based on BP neural network and chaotic system. *Multimedia Tools and Applications*, 79(27), 19963-19992. https://doi.org/10.1109/TCSVT.2018.2878026

[5]Ni, R., Wang, F., Wang, J., & Hu, Y. (2021). Multi-image encryption based on compressed sensing and deep learning in optical gyrator domain. *IEEE Photonics Journal*, 13(3), 1-16. https://doi.org/10.1109/JPHOT.2021.3076480

[6]Zhou, N., Zhang, A., Wu, J., Pei, D., & Yang, Y. (2014). Novel hybrid image compression–encryption algorithm based on compressive sensing. *Optik*, 125(18), 5075-5080. https://doi.org/10.1016/j.ijleo.2014.06.054

[7]Zhou, N., Pan, S., Cheng, S., & Zhou, Z. (2016). Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing. *Optics & Laser Technology*, 82, 121-133. https://doi.org/10.1016/j.optlastec.2016.02.018

[8]Zhou, N., Jiang, H., Gong, L., & Xie, X. (2018). Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging. *Optics and Lasers in Engineering*, 110, 72-79. https://doi.org/10.1016/j.optlaseng.2018.05.014

[9]Visually asymmetric image encryption algorithm based on SHA-3 and compressive sensing by embedding encrypted image. (2022). *Alexandria Engineering Journal*, 61(10), 7637-7647. https://doi.org/10.1016/j.aej.2022.01.015

[10]Chai, X., Gan, Z., Chen, Y., & Zhang, Y. (2017). A visually secure image encryption scheme based on compressive sensing. *Signal Processing*, 134, 35-51. https://doi.org/10.1016/j.sigpro.2016.11.016

[11]Xu, Q., Sun, K., He, S., & Zhu, C. (2020). An effective image encryption algorithm based on compressive sensing and 2D-SLIM. *Optics and Lasers in Engineering*, 134, Article 106178.

[12]Gan, Z., Bi, J., Ding, W., & Chai, X. (2021). Exploiting 2D compressed sensing and information entropy for secure color image compression and encryption. *Neural Computing and Applications*, 33(19), 12845-12867. https://doi.org/10.1007/s00521-021-05937-4

[13]Ghaffari, A. (2021). Image compression-encryption method based on two-dimensional sparse recovery and chaotic system. *Scientific Reports*, 11(1), 369. https://doi.org/10.1038/s41598-020-79747-4

[14]Li, P., & Lo, K.-T. (2018). A content-adaptive joint image compression and encryption scheme. *IEEE Transactions on Multimedia*, 20(8), 1960-1972. https://doi.org/10.1109/TMM.2017.2786860

[15]Li, P., & Lo, K.-T. (2019). Joint image encryption and compression schemes based on 16 × 16 DCT. *Journal of Visual Communication and Image Representation*, 58, 12-24. https://doi.org/10.1016/j.jvcir.2018.11.018

[16]Ballé, J., Minnen, D., Singh, S., Hwang, S. J., & Johnston, N. (2018). Variational image compression with a scale hyperprior. *International Conference on Learning Representations.*

[17]Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2021). Recent advances in the Internet-of-Medical-Things (IoMT) systems security. *IEEE Internet of Things Journal*, 8(11), 8707-8718.

[18]Lakshmi, T. N., Jyothi, S., & Kumar, M. R. (2021). Image Encryption Algorithms Using Machine Learning and Deep Learning Techniques—A Survey. *In Springer, Cham* (pp. 507-515).

[19]Ghadirli, H. M., Nodehi, A., & Enayatifar, R. (2019). An overview of encryption algorithms in color images. *Signal Processing*, 164, 163-185.

[20]Kaur, M., & Kumar, V. (2020). A comprehensive review on image encryption techniques. *Archives of Computational Methods in Engineering*, 27(1), 15-43.

[21]Yang, N., Zhang, S., Bai, M., & Li, S. (2022). Medical image encryption based on Josephus traversing and hyperchaotic Lorenz system. *Journal of Shanghai Jiaotong University*, 29(1), 91-108.

[22]Wang, T., & Wang, M.-H. (2020). Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding. *Optics and Laser Technology*, 132, 106355.

[23]Sang, Y., Sang, J., & Alam, M. S. (2022). Image encryption based on logistic chaotic systems and deep autoencoder. *Pattern Recognition Letters*, 153, 59-66.

[24]Sun, X., & Chen, Z. (2022). A new image encryption strategy based on Arnold transformation and logistic map. In Proceedings of the *11th International Conference on Computer Engineering and Networks* (pp. 712-720). Springer, Singapore.

[25]Pak, C., & Huang, L. (2017). A new color image encryption using combination of the 1D chaotic map. *Signal Processing*, 138, 129-137.

[26]Tang, J., Zhang, F., & Ni, H. (2023). A novel fast image encryption scheme based on a new one-dimensional compound sine chaotic system. *The Visual Computer*, 39(10), 4955-4983.

[27]R. Ch, M. Radha, M. Mahendar, and P. Manasa, "A Comparative Analysis for Deep-Learning-Based Approaches for Image Forgery Detection," *International Journal of Systematic Innovation*, 8(1),1–10, 2024.

[28]Zhu, S., Deng, X., Zhang, W., & Zhu, C. (2023). Secure image encryption scheme based on a new robust chaotic map and strong S-box. *Mathematics and Computers in Simulation*, 207, 322-346.

[29]Wang, F., Sang, J., Huang, C., Cai, B., Xiang, H., & Sang, N. (2022). Applying deep learning to known-plaintext attack on chaotic image encryption schemes. *In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)* (pp. 3029-3033).

[30]Panwar, K., Kukreja, S., Singh, A., & Singh, K. K. (2023). Towards deep learning for efficient image encryption. *Procedia Computer Science*, 218, 644-650.

[31]Wang, C., & Zhang, Y. (2022). A novel image encryption algorithm with deep neural network. *Signal Processing*, 196, 108536.

[32]Man, Z., Li, J., Di, X., Sheng, Y., & Liu, Z. (2021). Double image encryption algorithm based on neural network and chaos. *Chaos, Solitons & Fractals*, 152, 111318.

[33]Maniyath, S. R., & Thanikaiselvan, V. (2020). An efficient image encryption using deep neural network and chaotic map. *Microprocessors and Microsystems*, 77, 103134.

[34]R. Ch, M. Sridevi, M. Ramchander, V. Ramesh, and V. P. Kumar, "Enhancing Digital Security Using Signa-Deep for Online Signature Verification and Identity Authentication," *International Journal of Systematic Innovation*, vol. 8, no. 2, pp. 58–69, 2024.

[35]Zhou, S., Zhao, Z., & Wang, X. (2022). Novel chaotic colour image cryptosystem with deep learning. *Chaos, Solitons & Fractals*, 161, 112380.

[36]BACAK, A., ŞENEL, M., & GÜNAY, O. (2023). Convolutional Neural Network (CNN) Prediction on Meningioma, Glioma with Tensorflow. *International Journal of Computational and Experimental Science and Engineering*, 9(2), 197–204. Retrieved from https://ijcesen.com/index.php/ijcesen/article/view/210

[37]Johnsymol Joy, & Mercy Paul Selvan. (2025). An efficient hybrid Deep Learning-Machine Learning method for diagnosing neurodegenerative disorders. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.701

[38]Sreetha E S, G Naveen Sundar, & D Narmadha. (2024). Enhancing Food Image Classification with Particle Swarm Optimization on NutriFoodNet and Data Augmentation Parameters. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.493

[39]P, P., P, D., R, V., A, Y., & Natarajan, V. P. (2024). Chronic Lower Respiratory Diseases detection based on Deep Recursive Convolutional Neural Network. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.513

[40]U. S. Pavitha, S. Nikhila, & Mohan, M. (2024). Hybrid Deep Learning Based Model for Removing Grid-Line Artifacts from Radiographical Images. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.514

[41]Radhi, M., & Tahseen, I. (2024). An Enhancement for Wireless Body Area Network Using Adaptive Algorithms. *International Journal of Computational and Experimental Science and Engineering*, 10(3). https://doi.org/10.22399/ijcesen.409

[42]Jha, K., Sumit Srivastava, & Aruna Jain. (2024). A Novel Texture based Approach for Facial Liveness Detection and Authentication using Deep Learning Classifier. *International Journal of Computational and Experimental Science and Engineering*, 10(3). https://doi.org/10.22399/ijcesen.369

[43]Boddupally JANAIAH, & Suresh PABBOJU. (2024). HARGAN: Generative Adversarial Network

BasedDeep Learning Framework for Efficient Recognition of Human Actions from Surveillance Videos. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.587

[44]Sashi Kanth Betha. (2024). ResDenseNet:Hybrid Convolutional Neural Network Model for Advanced Classification of Diabetic Retinopathy(DR) in Retinal Image Analysis. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.693

[45]T. Deepa, & Ch. D. V Subba Rao. (2025). Brain Glial Cell Tumor Classification through Ensemble Deep Learning with APCGAN Augmentation. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.803

[46]Bolleddu Devananda Rao, & K. Madhavi. (2024). BCDNet: A Deep Learning Model with Improved Convolutional Neural Network for Efficient Detection of Bone Cancer Using Histology Images. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.430

[47]URAL, A., & KİLİMCİ, Z. H. (2021). The Prediction of Chiral Metamaterial Resonance using Convolutional Neural Networks and Conventional Machine Learning Algorithms. *International Journal of Computational and Experimental Science and Engineering*, 7(3), 156–163. Retrieved from https://ijcesen.com/index.php/ijcesen/article/view/165